Therefore, I claim:

1. In a system comprising a server and a computer communicatively connected together via an HTTP-based network, a method of establishing by the server a secure state between the server and a user operating the computer, said method comprising:

receiving, from the computer, a user key comprising U bits, where U > 0;

creating, from said user key, a cryptographic key;

encrypting, using said cryptographic key, user data;

storing the encrypted user data in a cookie;

naming the cookie by assigning name data to the cookie;

sending the cookie to the computer for storage thereby;

receiving the cookie from the computer;

receiving said user key from the computer;

recreating, from said user key, said cryptographic key;

extracting the encrypted user data from the cookie;

decrypting, using said cryptographic key, the encrypted user data; and

establishing the secure state between the server and the user based on the decrypted user data.

2. The method of claim 1, further comprising

before said encrypting, receiving user information from the computer;

wherein the user data is based on the user information.

3. The method of claim 1, wherein creating said cryptographic key comprises inserting at least one bit at a position K of said user key, where $1 \leq K \leq U+1$, and recreating said cryptographic key comprises inserting the at least one bit at the position K of said user key.

4. The method of claim 1, wherein creating said cryptographic key comprises deleting I bits from said user key from a position K of said user key, where $1 \leq I < U$ and $1 \leq K \leq (U - I + 1)$, and recreating said cryptographic key comprises deleting the I bits from said user key from the position K of said user key.

5. The method of claim 1, further comprising:

before encrypting, seeding the user data according to a format;

wherein the secure state is established if the decrypted user data is seeded according to the format.

6. The method of claim 5, further comprising:

sending, to the computer, an error message if the decrypted user data is not seeded according to the format.

7. In a system comprising a server and a computer communicatively connected together via an HTTP-based network, a method of establishing by the server a secure state between the server and a user operating the computer, said method comprising:

receiving, from the computer, a cookie comprising encrypted user data that may be seeded according to a format;

receiving a user key from the computer;

creating, from said user key, a cryptographic key;

extracting the encrypted user data from said cookie;

decrypting, using said cryptographic key, the encrypted user data; and

establishing the secure state between the server and the user based on the decrypted user data.

8. The method of claim 7, wherein creating said cryptographic key comprises inserting at least one bit at a position K of said user key, where $1 \leq K \leq U+1$.

9. The method of claim 7, wherein creating said cryptographic key comprises deleting I bits from said user key from a position K of said user key, where $1 \leq I < U$ and $1 \leq K \leq (U - I + 1)$.

10. The method of claim 7, wherein the secure state is established if the decrypted user data is seeded according to the format.

11. The method of claim 10, further comprising:

sending, to the computer, an error message if the decrypted user data is not seeded according to the format.

12. For use by a server communicatively connected to a computer via an HTTP-based network, a computer readable medium comprising instructions for establishing a secure state between the server and a user operating the computer, by causing the server to perform actions, comprising:

receiving, from the computer, a user key comprising U bits, where $U > 0$;

creating, from said user key, a cryptographic key;

encrypting, using said cryptographic key, user data;

storing the encrypted user data in a cookie;

naming the cookie by assigning name data to the cookie;

sending the cookie to the computer for storage thereby;

receiving the cookie from the computer;

receiving said user key from the computer;

recreating, from said user key, said cryptographic key;

extracting the encrypted user data from the cookie;

decrypting, using said cryptographic key, the encrypted user data; and

establishing the secure state between the server and the user based on the decrypted user data.

13. The computer readable medium of claim 12, wherein the actions further comprise:

before said encrypting, receiving user information from the computer;

wherein at least a portion of the user data is based on the user information.

14. The computer readable medium of claim 12, wherein creating said cryptographic key comprises inserting at least one bit at a position K of said user key, where $1 \leq K \leq U+1$, and recreating said cryptographic key comprises inserting the at least one bit at the position K of said user key.

15. The computer readable medium of claim 12, wherein creating said cryptographic key comprises deleting I bits from said user key from a position K of said user key, where $1 \leq I < U$ and $1 \leq K \leq (U - I + 1)$, and recreating said cryptographic key comprises deleting the I bits from said user key from the position K of said user key.

16. The computer readable medium of claim 12, wherein the actions further comprise:

before encrypting, seeding the user data according to a format;

wherein the secure state is established if the decrypted user data is seeded according to the format.

17. The computer readable medium of claim 16, wherein the actions further comprise:

sending, to the computer, an error message if the decrypted user data is not seeded according to the format.

18. For use by a server communicatively connected to a computer via an HTTP-based network, a computer readable medium comprising instructions for establishing a secure state between the server and a user operating the computer, by causing the server to perform actions, comprising:

receiving, from the computer, a cookie comprising encrypted user data that may be seeded according to a format;

receiving a user key from the computer;

creating, from said user key, a cryptographic key;

extracting the encrypted user data from said cookie;

decrypting, using said cryptographic key, the encrypted user data; and

establishing the secure state between the server and the user based on the decrypted user data.

19. The computer readable medium of claim 18, wherein creating said cryptographic key comprises inserting at least one bit at a position K of said user key, where $1 \leq K \leq U+1$.

20. The computer readable medium of claim 18, wherein creating said cryptographic key comprises deleting I bits from said user key from a position K of said user key, where $1 \leq I < U$ and $1 \leq K \leq (U - I + 1)$.

21. The computer readable medium of claim 18, wherein the secure state is established if the decrypted user data is seeded according to the format.

22. The computer readable medium of claim 21, wherein the actions further comprise:

sending, to the computer, an error message if the decrypted user data is not seeded according to the format.